Počítačové sítě

Studijní text pro septimu a 3. ročník gymnázia

Bc. Tomáš Kysela

Gymnázium J. S. Machara, Brandýs nad Labem – Stará Boleslav



Předmluva

Předkládaný studijní text vznikl z potřeby poskytnout studentům vyššího gymnázia ucelený materiál, který by překlenul propast mezi běžnou středoškolskou informatikou a vysokými nároky vysokoškolského studia. Většina dostupné středoškolské literatury se v kontextu počítačových sítí omezuje na povrchní popis uživatelské konfigurace, zatímco plnohodnotné akademické publikace často předpokládají hlubokou znalost pokročilého matematického aparátu. Skripta si proto kladou za cíl nalézt optimální průsečík. Odklánějí se od pouhého memorování protokolů a budují pochopení síťových architektur přímo od jejich fyzikálních a matematických základů.

Text představuje primárně podpůrný studijní materiál k prezenční výuce. Jeho struktura a odborný rozsah jsou však koncipovány tak, aby plně vyhovovaly i nárokům na samostatné studium či hlubší fixaci probrané látky. Závěrem je nutné podotknout, že v případě jakýchkoliv obsahových či terminologických diskrepancí mezi těmito skripty a ústním výkladem má vždy absolutní prioritu výklad vyučujícího.

Obsah

Předmluva 2
1. Matematický a fyzikální aparát 4
   1.1. Jednotky 4
      1.1.1. Standardizace předpon (SI vs. IEC) 4
   1.2. Číselné soustavy 4
   1.3. Vybrané matematické funkce 6
      1.3.1. Exponenciální a logaritmické funkce 6
      1.3.2. Goniometrické funkce a harmonický signál 7
2. Směrování v sítích 7
   2.1. Hierarchická struktura adres 8
   2.2. IP adresa 8
      2.2.1. IPv4 9
      2.2.2. IPv6 10
Přílohy 13
Použitá literatura 14

1. Matematický a fyzikální aparát

Než začneme se samotným učivem, je třeba zopakovat znalosti předchozích let. Mezi ty, které budeme potřebovat nejvíce, patří zajisté převody jednotek a číselných soustav, znalost základních pojmů počítačové terminologie a základy fyziky a matematiky v rozsahu učiva prvních dvou ročníků střední školy. Jelikož znalost těchto pojmů je u studentů často neunifikovaná, pojďme se podívat na jednotlivá odvětví v tomto textu.

1.1. Jednotky

Základní a dále nedělitelnou jednotkou informace v binárních systémech je jeden **bit** (značíme malým b). Tato jednotka reprezentuje množství informace získané odpovědí na jednu otázku typu ano/ne, respektive nabývá logických hodnot 0 nebo 1. Vyšším logickým celkem je **byte** (případně **oktet**, značíme velkým B), definovaný jako uspořádaná osmice bitů ($1\,\mathrm{B} = 8\,\mathrm{b}$).

Zatímco datové kapacity úložných systémů jsou tradičně vyjadřovány v bytech, propustnost komunikačních kanálů (přenosová rychlost) je v telekomunikacích striktně definována v **bitech za sekundu** ($\mathrm{b\,s^{-1}}$).

1.1.1. Standardizace předpon (SI vs. IEC)

V technické praxi dochází k častým diskrepancím při označování řádových násobků datových jednotek. Pro korektní vyjadřování je nutné rozlišovat dva normované systémy:

1. **Desítkové předpony (Soustava SI)**: Vycházejí z Mezinárodní soustavy jednotek, která je standardem ve fyzice a technických oborech. V telekomunikacích a síťovém inženýrství se tyto předpony (mocniny deseti) využívají striktně ke kvantifikaci přenosových rychlostí.
   - 1 bit (b) = $10^0\ \mathrm{b} = 1\,\mathrm{b}$
   - 1 kilobit (kb) = $10^3\ \mathrm{b} = 1000\,\mathrm{b}$
   - 1 megabit (Mb) = $10^6\ \mathrm{b} = 1\,000\,000\,\mathrm{b}$
   - 1 gigabit (Gb) = $10^9\ \mathrm{b} = 1\,000\,000\,000\,\mathrm{b}$
2. **Binární předpony (Standard IEC 60027-2)**: Využívány v informatice pro kvantifikaci kapacity pamětí (RAM) a velikosti souborů v operačních systémech. Jedná se o mocniny dvou.
   - 1 kibibyte (KiB) = $2^{10}\ \mathrm{B} = 1024\,\mathrm{B}$
   - 1 mebibyte (MiB) = $2^{20}\ \mathrm{B} = 1\,048\,576\,\mathrm{B}$
   - 1 gibibyte (GiB) = $2^{30}\ \mathrm{B} = 1\,073\,741\,824\,\mathrm{B}$

1.2. Číselné soustavy

Pro hluboké porozumění fungování výpočetní techniky a datových přenosů je naprosto nezbytné ovládnout principy pozičních číselných soustav. Z matematického hlediska je poziční číselná soustava definována svým základem, neboli radixem, který určuje počet unikátních číslic používaných k reprezentaci hodnot. Hodnota každé číslice v daném zápisu je přímo závislá na její konkrétní pozici vůči řádové čárce.

Definice (Poziční číselná soustava): Poziční číselná soustava o základu $b \in \mathbb{N}, b \geq 2$, umožňuje jednoznačný zápis libovolného reálného čísla N pomocí lineární kombinace mocnin základu b. Matematicky lze celkovou hodnotu čísla vyjádřit polynomem ve tvaru sumy:

$$N = \sum_{i=-m}^{n-1} a_i \cdot b^i \tag{1}$$

V rovnici 1 zastupuje proměnná n počet celočíselných řádů, m označuje počet desetinných, respektive zlomkových řádů a koeficienty a_i představují platné číslice dané soustavy. Pro každou číslici přitom musí striktně platit nerovnost $0 \leq a_i < b$.

Příklad k rozmyšlení: Definice výše dává smysl i pro $b = 1$, ačkoli název *poziční soustava* může být trochu zavádějící. Rozmyslete si, jaké vlastnosti taková *unární* soustava má a jak se rychle mezi ní a desítkovou převádí.

Nejrozšířenějším systémem v běžném lidském životě je desítková, tedy dekadická soustava. Její základ tvoří číslo deset a k zápisu využívá číslice nula až devět. Pro moderní číslicové obvody a datové sítě je však dekadická soustava z fyzikálního i inženýrského hlediska zcela nevhodná. Konstrukce hardwaru, který by spolehlivě rozlišoval deset různých napěťových úrovní na komunikačním médiu, by byla neúměrně složitá a především extrémně náchylná k chybám způsobeným vnějším elektromagnetickým šumem.

Z tohoto důvodu je veškerá výpočetní technika a datová komunikace na své nejnižší vrstvě postavena výhradně na dvojkové, neboli binární soustavě. Základem této soustavy je číslo dvě a využívají se pouze číslice nula a jedna. Tyto dva diskrétní stavy lze ve fyzické vrstvě snadno, levně a s maximální možnou spolehlivostí reprezentovat jako dvě různé úrovně elektrického napětí či odlišné fáze elektromagnetického signálu. Aplikaci obecného rozvoje z rovnice 1 na binární systém lze demonstrovat na převodu čtyřbitového čísla do dekadické formy:

$$1101_2 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 13_{10} \tag{2}$$

Ačkoliv je binární zápis demonstrativně ukázaný v rovnici 2 pro stroje naprosto přirozený a z hlediska návrhu logických obvodů optimální, pro člověka se stává u větších čísel zcela nepřehledným z důvodu extrémní délky zápisu. Aby se předešlo lidským chybám při interpretaci dlouhých binárních sekvencí v diagnostických nástrojích a síťových analyzátorech, zavedla se do informatiky šestnáctková, neboli hexadecimální soustava. Její základ činí šestnáct, což nevyhnutelně vyžaduje použití šestnácti unikátních symbolů, kde hodnoty deset až patnáct reprezentují písmena latinské abecedy A až F.

Klíčová výhoda hexadecimální soustavy nespočívá ve faktu, že by s ní počítače přímo pracovaly, nýbrž v jejím dokonalém matematickém vztahu k soustavě binární. Tento vztah primárně vyplývá z rovnosti základu obou soustav:

$$b_{\text{hex}} = (b_{\text{bin}})^4 \rightarrow 16 = 2^4 \tag{3}$$

Z algebraické vlastnosti popsané v rovnici 3 přímo plyne matematický důsledek, že právě jedna hexadecimální číslice dokáže reprezentovat přesně čtyři bity, tedy jeden takzvaný nibble neboli půlbyte. Dvě hexadecimální číslice tak vždy tvoří přesně jeden byte. Tato skutečnost umožňuje inženýrům triviální a velmi rychlou vizuální konverzi mezi binárním a hexadecimálním zápisem bez nutnosti složitých výpočtů. Hexadecimální soustava tak slouží jako ideální kompromis poskytující kompaktní a člověkem snadno čitelný zápis.

1.3. Vybrané matematické funkce

Matematický aparát představuje integrální součást všech informatických disciplín. V rámci počítačových sítí se na vyšších vrstvách referenčních modelů uplatňuje mimo jiné v podobě pokročilých směrovacích algoritmů, výpočtů kontrolních součtů pro zajištění integrity dat či při nasazení asymetrické kryptografie. Pro pochopení samotných elementárních základů síťové komunikace, tedy logické adresace uzlů a fyzického přenosu signálu, je však nezbytné bezpečně ovládat několik specifických matematických funkcí.

Zatímco exponenciální funkce slouží primárně ke kvantifikaci a návrhu rozsahů adresních prostorů, logaritmy a goniometrické funkce jsou klíčové pro analýzu na fyzické vrstvě. Právě na této nejnižší úrovni dochází k transformaci abstraktních logických bitů na měřitelné fyzikální veličiny, jakými jsou změny elektrického napětí, optického výkonu nebo intenzity elektromagnetického pole.

1.3.1. Exponenciální a logaritmické funkce

Z matematického hlediska je exponenciální funkce definována předpisem $f(x) = a^x$, kde základ a je kladné reálné číslo různé od jedné a nezávislá proměnná x se nachází v exponentu. Charakteristickou vlastností této třídy funkcí je dynamika jejího růstu. V kontextu výpočetní techniky a počítačových sítí má stěžejní význam exponenciální funkce o základu dvě ($a = 2$), jež přirozeně odráží binární charakter fyzické vrstvy číslicových systémů.

Tato specifická funkce definuje mimo jiné mohutnost adresního prostoru. Disponuje-li síťový protokol n-bitovým adresním polem, je schopen jednoznačně identifikovat množinu unikátních koncových uzlů, jejíž maximální velikost N je dána vztahem:

$$N = 2^n \tag{4}$$

Jak přímo vyplývá z rovnice 4, přidáním jediného bitu do adresního pole dochází k exponenciálnímu zdvojnásobení celkového počtu adresovatelných uzlů.

Inverzní operací k exponenciální funkci je logaritmus. Z matematického hlediska představuje logaritmus kladného reálného čísla x při základu a (kde $a > 0$ a $a \neq 1$) takový exponent y, na který je nutné umocnit základ a pro dosažení hodnoty x. Tento fundamentální vztah lze vyjádřit formální ekvivalencí:

$$y = \log_a x \Leftrightarrow a^y = x \tag{5}$$

V síťovém inženýrství se následně aplikují primárně dva specifické typy logaritmů. Logaritmus o základu dvě se uplatňuje v teorii informace, a to zejména při výpočtech informační

entropie a limitní kapacity kanálu. Dekadický logaritmus naproti tomu slouží k vyjádření poměru dvou výkonů pomocí bezrozměrné logaritmické jednotky decibel.

Definice (Decibel): Logaritmická míra útlumu, případně zisku, je definovaná jako desetinásobek dekadického logaritmu poměru výstupního výkonu P_{out} ku vstupnímu výkonu P_{in}. Matematicky je útlum L v decibelech definován vztahem:

$$L = 10 \cdot \log_{10}\left(\frac{P_{\text{out}}}{P_{\text{in}}}\right) \tag{6}$$

Využitím rovnice 5 a dosazením do definice v rovnici 6 lze snadno odvodit, že pokles výkonu signálu na polovinu původní hodnoty na přenosovém médiu odpovídá útlumu přibližně -3 dB, zatímco pokles na setinu odpovídá -20 dB.

1.3.2. Goniometrické funkce a harmonický signál

Goniometrické funkce, primárně sinus a kosinus, představují v matematice elementární nástroj pro popis periodických a kmitavých dějů. Jejich oborem hodnot je uzavřený interval $[-1, 1]$, což z nich činí ideální model pro reprezentaci vlnění. V kontextu počítačových sítí hrají tyto spojité funkce nezastupitelnou roli při fyzickém přenosu informací, neboť tvoří matematický fundament nosných vln.

Digitální data vygenerovaná koncovým uzlem nelze do přenosového média obvykle odeslat v jejich nativní formě diskrétních pravoúhlých pulzů. Takový signál je totiž v reálném fyzikálním médiu vysoce náchylný k deformaci tvaru a na delších vzdálenostech podléhá silnému útlumu, což znemožňuje spolehlivou detekci původních dat na straně příjemce. Z tohoto důvodu se informace, a to primárně v bezdrátových sítích a na optických trasách, modulují na nosnou vlnu, která má charakter spojitého harmonického signálu.

Definice (Harmonický signál): Základní harmonický signál v čase t je plně popsán transformovanou goniometrickou funkcí sinus:

$$u(t) = A_m \cdot \sin(2\pi f t + \varphi) \tag{7}$$

V rovnici 7 reprezentuje parametr A_m maximální amplitudu signálu, proměnná f označuje frekvenci udávanou v jednotkách hertz (Hz) a symbol φ definuje počáteční fázový posuv.

Diskrétní modulační techniky následně kódují přenášené binární informace do nosné vlny cílenou a přesně definovanou změnou jednoho nebo více z těchto tří volných parametrů v čase.

2. Směrování v sítích

Z technických a ekonomických důvodů je v moderních rozlehlých sítích, čítajících miliony až miliardy koncových uzlů, zcela nerealizovatelné, aby bylo každé zařízení fyzicky propojeno

s každým dalším systémem. Z tohoto důvodu je nutné budovat síťovou infrastrukturu jako množinu sdílených, vzájemně propojených mezilehlých uzlů. Návrh topologie takové sítě musí představovat optimální kompromis: na jedné straně musí minimalizovat celkový počet prvků a propojovacích okruhů, na straně druhé však musí poskytovat dostatečnou redundanci a robustnost pro bezvýpadkové překonání poruchy jednotlivých linek či zařízení.

K efektivnímu fungování takto rozsáhlé infrastruktury se využívá abstrakce ve formě samotného směrování. V tomto modelu není nezbytné, aby odesílatel nebo jakýkoliv dílčí uzel předem znal kompletní cestu k finální destinaci. Zcela postačuje, když každý aktivní prvek v síti disponuje informací o tom, jakému nejbližšímu sousednímu uzlu má přijatou zprávu topologicky předat.

2.1. Hierarchická struktura adres

Aby mohl libovolný síťový uzel plnit svou primární směrovací funkci, musí primárně disponovat mechanismem pro rozhodování o optimálním směru odeslání přijatých dat. Za tímto účelem si každý aktivní prvek v topologii, a to jak koncový systém, tak především mezilehlý směrovač, udržuje strukturované informace o svých přímých sousedech a topologickém směru k dalším uzlům, přičemž tato klíčová provozní data jsou trvale ukládána ve formě takzvané směrovací tabulky. Ačkoliv by z čistě teoretického hlediska bylo nejefektivnější, pokud by každý uzel disponoval absolutní znalostí o přesné poloze všech ostatních zařízení, v kontextu globálního internetu s miliardami koncových stanic je tento plochý adresní model z důvodu extrémních nároků na paměťový prostor a výpočetní výkon zcela nerealizovatelný.

K vyřešení tohoto fundamentálního problému se v rozlehlých sítích obligatorně implementuje hierarchická struktura adres. Tento přístup je založen na principu logického seskupování těch koncových stanic, jež sdílejí totožnou počáteční část své síťové adresy a nacházejí se ve stejné logické podsíti. Díky této adresní korelaci zcela postačuje, aby globální směrovače udržovaly ve svých tabulkách pouze jediný agregovaný záznam reprezentující dosažitelnost celé této rozsáhlé skupiny. Jakmile je datový dotaz doručen ke hraničnímu uzlu (vstupnímu bodu) dané cílové podsítě, další doručování již probíhá na ryze lokální úrovni, kde jednotlivé uzly detailně znají svou vzájemnou topologickou polohu a bezpečně dopraví informaci k finálnímu příjemci.

2.2. IP adresa

Při každé komunikaci je třeba adresovat náš cíl, ať již v tradiční poštovní korespondenci, kde má každý dům svoji unikátní adresu, tak v telefonické, kde máme unikátní telefonní čísla, tak i zde, v počítačových sítích, kde se využívá tzv. IP adresa. Všechny tyto adresy zároveň splňují dvě základní vlastnosti: jsou unikátní a jsou hierarchické. Jako ukázku hierarchie lze použít onu poštovní adresu, například *Královická 668, 250 01 Brandýs nad Labem - Stará Boleslav, Česká republika*. Nejširší skupinou je právě Česká republika, následně zúžena na město/pobočku České pošty, ulici a nakonec číslo popisné.

Architekturu a přesný formát IP adres specifikují standardizační dokumenty organizace IETF (Internet Engineering Task Force), takzvané RFC (Request for Comments). V současné síťové infrastruktuře koexistují dva dominantní standardy: historicky starší protokol IPv4, defino-

vaný dokumentem RFC 791° ze září 1981, a moderní protokol IPv6, jehož specifikace byla ukotvena v RFC 2460° z prosince 1998.

Existence a paralelizace těchto dvou odlišných norem je důsledkem historického vývoje. Předchozí verze protokolu (0 až 3) sloužily mezi lety 1977 a 1979 primárně jako vývojové a experimentální. Verze 5 (Internet Stream Protocol) pak představovala první pokusy o implementaci protokolu optimalizovaného pro přenos streamovaného zvuku a videa, avšak nikdy nedosáhla masového komerčního nasazení. Do praxe tak přešly výhradně verze 4 a 6, které budou detailněji rozebrány v následujících podkapitolách.

2.2.1. IPv4

Definice (IPv4 adresa): Adresa protokolu IP verze 4 je definována jako 32-bitové pole. Pro usnadnění lidské čitelnosti a konfigurace se tento binární zápis standardně transformuje do takzvané tečkové notace. Celý dvaatřicetibitový adresní prostor je logicky rozdělen do čtyř osmibitových bloků (oktetů), přičemž každý oktet je reprezentován dekadickou hodnotou v uzavřeném intervalu od 0 do 255 a od sousedních oktetů je striktně oddělen symbolem tečky.

Tento strukturovaný formát zápisu lze názorně demonstrovat na následujícím příkladu, který ukazuje korelaci mezi běžně používanou dekadickou tečkovou notací a její skutečnou binární reprezentací v síťovém hardwaru:

10 . 3 . 14 . 6

`00001010 . 00000011 . 00001110 . 00000110`

Celkový počet unikátních kombinací, které lze z tohoto 32-bitového pole teoreticky vytvořit, definuje maximální mohutnost adresového prostoru. V případě protokolu IPv4 tak lze adresovat maximálně $2^{32} = 4\,294\,967\,296$ unikátních síťových uzlů.

Ačkoliv teoretická hodnota přesahující čtyři miliardy adres vypadala v raných fázích budování internetu jako zcela dostačující, již počátkem devadesátých let dvacátého století se začalo projevovat hrozící vyčerpání tohoto prostoru. Zásadním problémem nebylo pouze samotné exponenciálně rostoucí množství připojovaných zařízení, nýbrž historicky neefektivní a hrubý model přidělování, který vedl k masivnímu plýtvání dostupnými bloky IP adres. V původním návrhu protokolu se totiž adresový prostor dělil do pěti striktních kategorií, takzvaných tříd, které se standardně označují písmeny A, B, C, D a E.

Příslušnost konkrétní IP adresy k dané třídě byla vždy pevně determinována hodnotou jejích nejvyšších bitů v prvním oktetu, což následně uvnitř samotné struktury adresy striktně definovalo, jak dlouhá část slouží jako globální identifikátor sítě a jaký prostor zbývá pro adresaci koncového zařízení. Zatímco pro běžný síťový provoz byly určeny výhradně první tři jmenované třídy, přičemž třída A byla se svým osmibitovým identifikátorem sítě a 24-bitovým prostorem pro uzly navržena pro obří infrastruktury, třída B představovala kompromisní variantu pro střední instituce s rovnoměrným rozdělením šestnácti bitů pro obě části a třída

C naopak sloužila sítím s malým počtem uzlů, kde identifikátor sítě zabíral první tři oktety a pro adresaci koncových zařízení zbýval pouze oktet poslední.

Zbývající dvě kategorie měly v síťové architektuře vysoce specializované využití, neboť třída D byla vyhrazena výhradně pro takzvaný skupinový neboli multicastový provoz a třída E sloužila čistě pro experimentální účely a akademický výzkum. Nad rámec tohoto historického třídního dělení však pro protokol IPv4 platí další fundamentální pravidlo určující, že ne všechny syntakticky vygenerované adresy v definovaném rozsahu smí být reálně přiděleny koncovým zařízením, což lze primárně demonstrovat na případu adresy, jejíž bitová část vyhrazená pro identifikátor stanice obsahuje výhradně logické nuly[. Právě taková specifická hodnota je totiž dedikována pro identifikaci samotné sítě či podsítě jakožto logického celku, v důsledku čehož je její reálné přidělení jakémukoliv konkrétnímu síťovému rozhraní hostitele striktně zakázáno.

K vymezení hranice mezi identifikátorem sítě a identifikátorem koncového zařízení v rámci 24-bitového prostoru se využívá takzvaná síťová maska, jež představuje doplňkový 32-bitový parametr formálně provázaný se samotnou IP adresou. Z matematického a strukturálního hlediska je tato maska definována jako nepřerušená sekvence logických jedniček zleva, které jednoznačně překrývají a definují síťovou část adresy, následovaná sekvencí logických nul, jež naopak vymezují prostor pro adresaci samotných hostitelských uzlů. Prostřednictvím hardwarové aplikace operace bitového logického součinu (AND) mezi konkrétní IP adresou a k ní příslušející síťovou maskou dokáže libovolný aktivní síťový prvek okamžitě izolovat adresu dané sítě, což představuje základní výpočetní mechanismus naprosto nezbytný pro efektivní vyhodnocování směrovacích tabulek. Pro usnadnění lidské čitelnosti a administrátorské konfigurace se maska standardně zapisuje buď ve shodné tečkové dekadické notaci jako samotná IP adresa, přičemž typickým příkladem je hodnota 255.255.255.0, nebo se uplatňuje modernější a kompaktnější notace využívající lomítka následovaného dekadickým číslem, jež vyjadřuje celkový počet jedničkových bitů v masce.

255 . 255 . 255 . 0

11111111 . 11111111 . 11111111 . 00000000

10 . 0 . 1 . 3 / 24

2.2.2. IPv6

Ačkoliv historické zavedení síťových masek a dalších dílčích optimalizačních mechanismů dočasně zpomalilo proces vyčerpávání dostupných IPv4 adres, exponenciální nárůst počtu globálně propojených zařízení nevyhnutelně vyústil v nutnost vývoje a plošné implementace zcela nového standardu, jenž by síťové infrastruktuře poskytl řádově rozsáhlejší adresní prostor. Organizace IETF z tohoto důvodu formálně standardizovala protokol IPv6, jehož primárním úkolem je nejen definitivně překonat kapacitní limity svého předchůdce, ale rovněž strukturálně optimalizovat proces směrování v páteřních sítích prostřednictvím efektivnějšího návrhu datové hlavičky paketu.

Definice (IPv6 adresa): Adresa protokolu IPv6 je definována jako 128-bitové logické pole, jež je z důvodu naprosté neudržitelnosti standardní dekadické tečkové notace při takto masivní datové délce zapisováno primárně prostřednictvím hexadecimální číselné soustavy. Tento 128-bitový prostor je logicky rozdělen do osmi 16-bitových bloků, přičemž každý z těchto bloků nabývá hodnot v uzavřeném intervalu od 0 do $FFFF$ a od sousedních segmentů je za všech okolností striktně oddělen symbolem dvojtečky.

Vzhledem k tomu, že plný hexadecimální zápis takto dimenzované adresy by byl pro jakoukoliv administrátorskou konfiguraci velmi zdlouhavý a vysoce náchylný k lidským chybám, zavádí samotný standard syntaktická pravidla pro její kompresi. Tato normalizovaná pravidla umožňují beztrestné vynechání všech počátečních nul v libovolném individuálním bloku a zároveň poskytují možnost nahradit právě jednu nejdelší souvislou sekvenci čistě nulových bloků symbolem dvou bezprostředně po sobě jdoucích dvojteček, čímž se vizuální reprezentace adresy radikálně zefektivňuje.

Tento mechanismus komprese lze názorně demonstrovat na následujícím příkladu, který vizualizuje transformaci plně rozepsané IPv6 adresy do jejího syntakticky korektního, maximálně zkráceného tvaru:

$$2001:0db8:0000:0000:0000:ff00:0042:8329$$

$$\mathbf{2001:db8::ff00:42:8329}$$

Příklad k rozmyšlení: Proč v komprimovaném zápisu dovolujeme použít :: nejvýše jednou?

Z hlediska celkové matematické mohutnosti generuje implementace tohoto 128-bitového modelu naprosto nepředstavitelný adresový prostor čítající přesně 2^{128} unikátních kombinací, což odpovídá hodnotě přibližně $3.4 \cdot 10^{38}$ možných identifikátorů. Takto obrovská a z lidského pohledu jen obtížně uchopitelná zásoba s vysokou jistotou eliminuje jakékoliv reálné hrozby nedostatku volných adres pro budoucí generace síťových technologií.

Na rozdíl od historické implementace v protokolu IPv4, kde se k vymezení síťové části tradičně uplatňovala explicitně zapisovaná paralelní maska, se v architektuře IPv6 od tohoto vizuálně redundantního formátu zcela upouští a pro definici hranice mezi identifikátorem sítě (takzvaným prefixem) a identifikátorem samotného koncového zařízení se využívá výhradně kompaktní notace takzvaného bezklasového směrování (CIDR). V rámci tohoto moderního strukturálního přístupu je délka síťové části vyjádřena prostým připojením symbolu lomítka bezprostředně za zkrácený hexadecimální zápis IP adresy, jež je bez mezery následováno dekadickou hodnotou, která numericky definuje celkový počet počátečních bitů pevně alokovaných pro síťový prefix. Vzhledem k bezprecedentní matematické mohutnosti 128-bitového adresního prostoru se jako standard pro koncové lokální sítě (LAN) ustálila jednotná délka prefixu */64*, což v inženýrské praxi znamená, že první polovina adresy slouží ke komplexnímu

směrování napříč internetem i vnitrofiremní infrastrukturou, zatímco zbývajících plných 64 bitů je vyhrazeno výlučně pro naprosto unikátní identifikaci konkrétního koncového zařízení, přičemž tento hostitelský identifikátor může být dokonce automaticky odvozen z jeho hardwarové MAC adresy.

Přílohy

A. Seznam použitých zkratek

Organizace

IETF — Internet Engineering Task Force*: Mezinárodní organizace zodpovědná za vývoj a standardizaci internetových protokolů.* 8, 10

Směrování

CIDR — Classless Inter-Domain Routing*: Beztřídní směrování umožňující flexibilní alokaci IP adres pomocí definice délky síťového prefixu.* 11

IPv4 — Internet Protocol verze 4*: Historicky nejrozšířenější protokol třetí vrstvy, který využívá 32-bitový adresní prostor rozdělený do 4 oktetů.* 3, 8, 9, 10, 11

IPv6 — Internet Protocol verze 6*: Moderní síťový protokol využívající 128-bitový adresní prostor zapisovaný v hexadecimální soustavě.* 3, 9, 10, 11

Použitá literatura

[1] L. Boháč a P. Bezpalec, *Datové sítě: přednášky*, 1. vyd. Praha: České vysoké učení technické, 2011.

[2] W. Odom, *Počítačové sítě bez předchozích znalostí*, 1. vyd. Brno: CP Books, 2005.

[3] R. Scott, *Networking for beginners: an easy guide to learning computer network basics*. United States: Independently published, 2019.

[4] I. Spurná, *Počítačové sítě: praktická příručka správce sítě*, 1. vyd. Kralice na Hané: Computer Media, 2010.